SSOAR

Open Access Repository
www.ssoar.info

Building resilient cyber-physical power systems: an approach using vulnerability assessment and resilience management

Tapia, Mariela; Thier, Pablo; Gößling-Reisemann, Stefan

Veröffentlichungsversion / Published Version
Zeitschriftenartikel / journal article

Empfohlene Zitierung / Suggested Citation:
Tapia, M., Thier, P., & Gößling-Reisemann, S. (2020). Building resilient cyber-physical power systems: an approach using vulnerability assessment and resilience management. *TATuP - Zeitschrift für Technikfolgenabschätzung in Theorie und Praxis / Journal for Technology Assessment in Theory and Practice*, *29*(1), 23-29. https://doi.org/10.14512/tatup.29.1.23

Nutzungsbedingungen:
Dieser Text wird unter einer CC BY Lizenz (Namensnennung) zur Verfügung gestellt. Nähere Auskünfte zu den CC-Lizenzen finden Sie hier:
https://creativecommons.org/licenses/by/4.0/deed.de

Terms of use:
This document is made available under a CC BY Licence (Attribution). For more Information see:
https://creativecommons.org/licenses/by/4.0

gesis Leibniz-Institut für Sozialwissenschaften

Mitglied der Leibniz-Gemeinschaft

Diese Version ist zitierbar unter / This version is citable under:
https://nbn-resolving.org/urn:nbn:de:0168-ssoar-68920-3

Building resilient cyber-physical power systems

An approach using vulnerability assessment and resilience management

Mariela Tapia, *Research Group Resilient Energy Systems, University of Bremen, Enrique-Schmidt-Str. 7, 28359 Bremen (mariela.tapia@uni-bremen.de)*
Pablo Thier, *Research Group Resilient Energy Systems, University of Bremen (thier@uni-bremen.de)*
Stefan Gößling-Reisemann, *Research Group Resilient Energy Systems, University of Bremen*

Power systems are undergoing a profound transformation towards cyber-physical systems. Disruptive changes due to energy system transition and the complexity of the interconnected systems expose the power system to new, unknown, and unpredictable risks. To identify the critical points, a vulnerability assessment was conducted, involving experts from the power as well as the information and communication technologies (ICT) sectors. Weaknesses were identified, e. g., the lack of policy enforcement, which are worsened by the unreadiness of the actors involved. Due to the complex dynamics of ICT, it is infeasible to keep a complete inventory of potential stressors to define appropriate preparation and prevention mechanisms. Therefore, we suggest applying a resilience management approach to increase the resilience of the system. It aims at better riding through failures rather than building higher walls. We conclude that building resilience in cyber-physical power systems is feasible and helps in preparing for the unexpected.

Die Gestaltung resilienter cyber-physischer Energiesysteme
Ein Ansatz basierend auf Vulnerabilitätsanalyse und Resilienzmanagement

Energiesysteme befinden sich in einem tiefgreifenden Wandel hin zu cyber-physischen Systemen. Disruptive Veränderungen, die von der Transformation des Energiesystems und der Komplexität der miteinander verbundenen Systeme herrühren, setzen das Stromnetz neuen, unbekannten Risiken aus. Mit einer Vulnerabilitätsanalyse unter Einbeziehung von Experten aus den Bereichen Energie und Informations- und Kommunikationstechnologien (IKT) wurden Schwachstellen identifiziert, z. B. Nachteile durch die fehlende Durchsetzung von Regulierungen, und eine mangelnde Anpassungsbereitschaft der beteiligten Akteure. Die komplexe IKT-Dynamik macht es unmöglich, potenzielle Stressoren vollständig zu erfassen, um geeignete Präventionsmechanismen zu definieren. Die vorgeschlagenen Resilienzmanagementmaßnahmen zielen darauf ab, Krisen besser zu bewältigen, anstatt auf höhere Barrieren zu setzen. Die Resilienz cyber-physikalischer Energiesysteme ist möglich.

This is an article distributed under the terms of the Creative Commons Attribution License CCBY 4.0 (https://creativecommons.org/licenses/by/4.0/)
https://doi.org/10.14512/tatup.29.1.23
Submitted: 23. 09. 2019. Peer reviewed. Accepted: 15. 01. 2020

Keywords: *cyber-physical power systems, resilience management, vulnerability assessment*

Introduction

Power systems are evolving through an extended convergence with information and communication technologies (ICT), leading to complex cyber-physical power systems (CPPS). This has brought opportunities to enhance the systems' performance and provide solutions to cope with the associated challenges of energy supply based on distributed and fluctuating renewable energies. However, cyber-attacks targeting power systems have been growing in number and sophistication in recent years. For instance, the attacks against the Ukrainian power grid in 2015 and 2016 that resulted in power outages (Dragos Inc. 2017). Another incident against a utility in the United States was reported on March 2019 (Sobzak 2019). Several risk and vulnerability assessments for power systems have been published in recent years (e. g. NIST 2014; Rossebo et al. 2017). In these studies, potential impacts and mitigation options were evaluated based on lists of potential threats and their likelihood of occurrence. We argue that due to the dynamic nature of ICT and its complex interdependency with the power infrastructure, we have to expect surprises. It will no longer be possible to identify a comprehensive inventory of potential threats, as is the case in classic risk management.

A reliable power supply is of great importance for almost all areas of life, therefore it is necessary to develop strategies that enable the power system to be prepared for expected and unexpected stressors. In other words, it is essential to apply a resilience management strategy. Many definitions of resilience exist in the scientific community (e. g. Jesse et al. 2019). For this study, we describe resilience as *a (socio-technical) system's ability to maintain its services under stress and in turbulent conditions* (Brand et al. 2017; Gleich et al. 2010). The advantage of using this definition is that it focusses on *the system services,* which must be outlined together with the stakeholders/us-

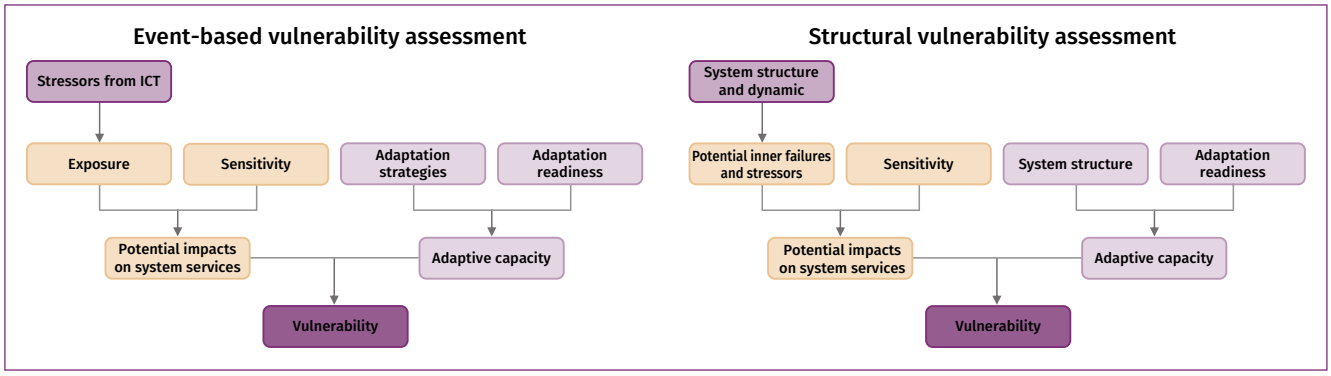

Fig. 1: Schematic representation of the VA methodology. **Left:** Event-based VA. **Right:** Structural VA.
Source: Authors' own compilation based on Gleich et al. (2010) and Gößling-Reisemann et al. (2013)

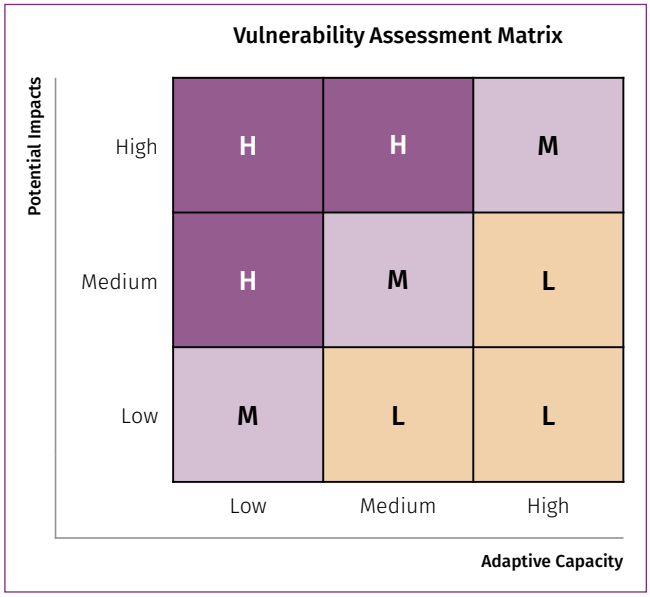

Fig. 2: Vulnerability assessment matrix that considers the level of potential impacts on system services and adaptive capacity. (**H**: High, **M**: Medium, **L**: Low).
Source: Authors' own compilation based on Gleich et al. (2010) and Gößling-Reisemann et al. (2013)

ers. In this way, changes and evolutions of the system are possible, which are core aspects of transitions. The focus lies on the complex nature of interconnectedness and interdependency, and the capability of the system to maintain its *services*.

This article presents the results of an empirical and interdisciplinary base study that involved actors from energy and ICT sectors through interviews and workshops, to get better insights into the vulnerabilities of CPPS. The study consists of two parts. First, a vulnerability assessment (VA) was performed to identify critical points coming from the ICT infrastructure. Second, a resilience strategy was developed by using a resilience management approach to identify how CPPS can be better prepared for any stressor.

Methodology

Vulnerability Assessment Approach

The event-based and structural VA methods (Fig. 1) carried out in Gleich et al. (2010) and Gößling-Reisemann et al. (2013) were used as reference for this study.

The potential impacts were evaluated based on their effect on the *system services,* which were defined in this case according to parameters for both the electric and ICT infrastructures. Regarding the electric infrastructure, the quantity criteria are determined by the system's ability to supply the connected load. The quality criteria are defined by direct technical parameters, such as power quality or reliability indices, and by indirect parameters, such as socio-economic and socioecological impacts. Regarding the ICT infrastructure, the approach considers the effect on the security requirements, i. e. confidentiality, integrity, availability and non-repudiation of data in transit or at rest (e. g. control commands, firmware, software, etc.).

The study focused on the German and European power system covering the complete electrical energy conversion chain and was limited to evaluate stressors from the ICT infrastructure. The component layer of the Smart Grid Architecture Model[1] was used as a reference architecture model. Two workshops and 19 semi-structured interviews were conducted with experts from the sectors: energy, industrial automation, ICT, and public bodies in the period between June 2016 to March 2017. The expert statements were evaluated by means of a comprehensive qualitative content analysis methodology based on Mayring (2014).

Combining the experts' opinions, relevant literature, and our own judgement, the potential impacts were qualitatively rated as high, medium or low according to the effects of stressors and structural weaknesses on the quality and quantity criteria of the system services. In order to determine the adaptive capacity, inputs from experts and literature were considered regarding existing or foreseen adaptation mechanisms and the readiness of the concerned actors to implement them. They were also qualita-

1 http://smartgridstandardsmap.com/

tively rated as high, medium or low. Consequently, the vulnerability level was the result of combining potential impacts and adaptive capacity according to the matrix showed in Fig. 2. A more detailed description on the VA methodology can be found in Tapia et al. (in press)

Resilience Management Approach

Resilient CPPS should have a diverse set of capabilities such as resistance/robustness, adaptation, innovation and improvisation to overcome known and unknown stressors. They help the systems to maintain their *system services* (see definition above). In this study, the resilience management approach described in Acatech et al. (2017) and Goessling-Reisemann and Thier (2019) was used as reference. It comprises a four-phase approach: (1) Prepare and prevent, (2) Implement robust and precautionary design, (3) Manage and recover from crises, and (4) Learn for the future. The suggested measures for each step were developed based on the VA results, the resilience design principles/elements described in Brand et al. (2017) and Goessling-Reisemann and Thier (2019), the statements of the interviewed experts, and our own judgments (Fig. 3).

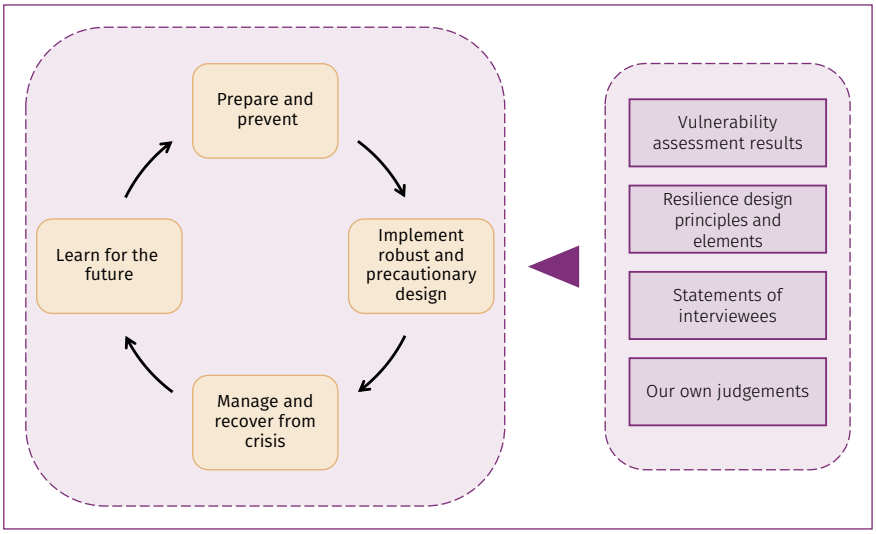

Fig. 3: Four phases of the resilient management approach scheme and the sources for determining the suggested measures for each phase. *Source: Authors' own compilation based on Acatech et al. (2017) and Goessling-Reisemann and Thier (2019)*

Vulnerability Assessment Results

The VA identified critical properties, structures and elements contributing to the vulnerability of the CPPS. Based on the qualitative content analysis results, the findings were sorted into the following four categories: (a) technology, (b) organizational security policies and procedures, (c) the human factor, and (d) regulations. Each category included subcategories and they were assessed individually using the VA methodology described above. All subcategories resulted in *high* vulnerability ratings following the combination of *medium to high* potential impacts with *medium or low* adaptive capacities (Tab. 1). The list of categories and subcategories is not intended to be comprehensive. However, it reflects the fact that the interviewees were queried about what the critical points are according to their opinion, which led to a list of high vulnerabilities. In the following section, the findings for each category will briefly be described.

Technology

The increased number of systems, endpoints and actors involved in the CPPS leads to a higher number of interconnections and communications. If these communications use unencrypted or

Category	Subcategory	Potential Impacts	Adaptive Capacity	Vulnerability
Technology	Insecure endpoints	M–H	M	**H**
	Insecure communications	M–H	M	**H**
Organizational security policies and procedures	Improper patch management	M–H	M	**H**
	Lack of interdisciplinary IT-OT knowledge	M–H	M	**H**
The human factor	Lack of security awareness in organizations	M–H	M	**H**
	Lack of security awareness among consumers	M–H	L	**H**
Regulations	Lack of effective implementation of standards and regulations	M–H	M	**H**
	Lack of coordinated effort to improve security	M–H	M	**H**

Tab. 1: Categories and subcategories that reflect critical properties, structures and elements of CPPS and the corresponding ratings of Potential Impacts, Adaptive Capacity and Vulnerability on the scale **L**: Low, **M**: Medium, **H**: High. *Source: Authors' own compilation based on Tapia et al. (in press)*

weakly encrypted network protocols, authentication keys and data payload are exposed (NIST 2014). Using Man-in-the-Middle attacks, threat agents will be able to listen, inject or manipulate messages between nodes. From one side, legacy communication protocols used in Industrial Control Systems (ICS) in the generation, transmission and distribution domains have evolved from proprietary point-to-point links and isolated from external networks to open and standard protocols. According to the experts, this represents a high security problem. The *'Crashoverride'* malware, which seems to have been used in the Ukraine blackout in 2016, is a good illustration of an advanced malware that leverages the weaknesses of certain ICS protocols (Dragos Inc. 2017).

From the other side, experts also stated that the more distributed and closer to the end-consumer the communication occurs, the more vulnerable it gets. The reason is that devices located at the customer premises (e. g. Internet-of-Things devices) are deployed with poor security features and furthermore, they are not regulated. In most of the cases, they do not have capabilities for secure key management, control access, or patch management. Security challenges and threats of smart home devices are discussed in Lee et al. (2014).

Organizational Security Policies and Procedures

Experts agreed that due to the increasing complexity and interdependencies between IT and Operation Technology (OT) infrastructures, the knowledge needed to address the new challenges has changed. In most of the cases, interdisciplinary knowledge is missing or limited, and therefore it is difficult to properly understand, design, implement and operate the complete complex system. Normally, OT assets are maintained by ICS operators and engineers rather than experienced IT professionals, which can result in common mistakes in maintenance, configuration, and lack of hardening (Bodungen et al. 2017). Moreover, typical IT systems security measures cannot be directly applied in ICS environments, because the process stability or availability could be affected. Therefore, specific and tailored security measures are needed.

As experts stated, ICS usually tend to be outdated, either because vendors do not provide security patches or because the particular system is time-critical. As a consequence, attackers are able to gain access to different system components by exploiting known security-gaps that have not yet been patched. Nevertheless, even if all patches and mitigations are kept up-to-date, attacks are becoming more sophisticated and adversaries use unknown zero-day exploits (McLaughlin et al. 2015), i. e. attacks based on previously unidentified and unpatched cyber-security gaps.

The Human Factor

The lack of effective security trainings and awareness programs in power sector organizations can lead to insufficiently trained or engaged personnel in cyber-security aspects (NIST 2014). Applying social engineering, threat agents are exploring new attack mechanisms targeting different levels in the organization. This is one of the fastest growing security problems according to the experts. In the Ukrainian blackout in 2015, attackers developed the *Blackenergy 3* tool malware and performed a phishing campaign targeting employees from the electricity distributor (Styzcynski and Beach-Westmoreland 2019).

Disgruntled employees, or ex-employees, who are not properly managed when leaving the company, may represent further potential threat actors. They could have detailed knowledge of the systems and access to critical data, allowing them to identify weak internal structures and methods to compromise the systems. Furthermore, critical information about the system configuration could be even publicly available through vendors' or asset owners' websites, employees' social media sites, or from other sources. Attackers can leverage this information for planning the attack.

Additionally, experts mentioned also that end users represent another vulnerable point because of their lack of awareness or understanding of the consequences of eventually low security of their smart devices. A more complex problem derives from end-users being prosumers, who may not have the expert-knowledge to implement and maintain appropriate security measures for Distributed Energy Resource (DER) systems (e. g. smart inverters).

Regulations

The lack of an effective implementation of security standards and regulations represents another critical point for CPPS. Experts considered that the absence of mandatory regulations to enforce power system operators to implement minimum required security standards, or vendors to provide the necessary security requirements in their products expose the system to possible cyber-attacks, for instance man-in-the-middle attacks on non-upgraded ICS systems running the IEC 60870-5 protocol (Maynard et al. 2014).

Different technical and organizational standards have been developed to address cyber-security requirements in smart grids (ENISA 2012; NIST 2014). Nevertheless, as experts stated, in most of the cases, these are only recommendations and the compliance to a minimum-security level is not enforced by regulations. Furthermore, the experts mentioned that there are no economic incentives for grid operators to invest in cyber-security enhancements. The decision to upgrade legacy ICS in order to implement the security measures could be delayed until the next planned lifecycle equipment replacement, not only because of the processes' criticality, but due to the additional associated costs. Another critical point, as experts remarked, is the missing effective coordination to improve security for the overall system.

The critical points discussed in this section are related to all categories mentioned above. The relationship is seen as lack of readiness of the involved actors to implement existing adaptation strategies. Thus, increasing the vulnerability level of each category itself.

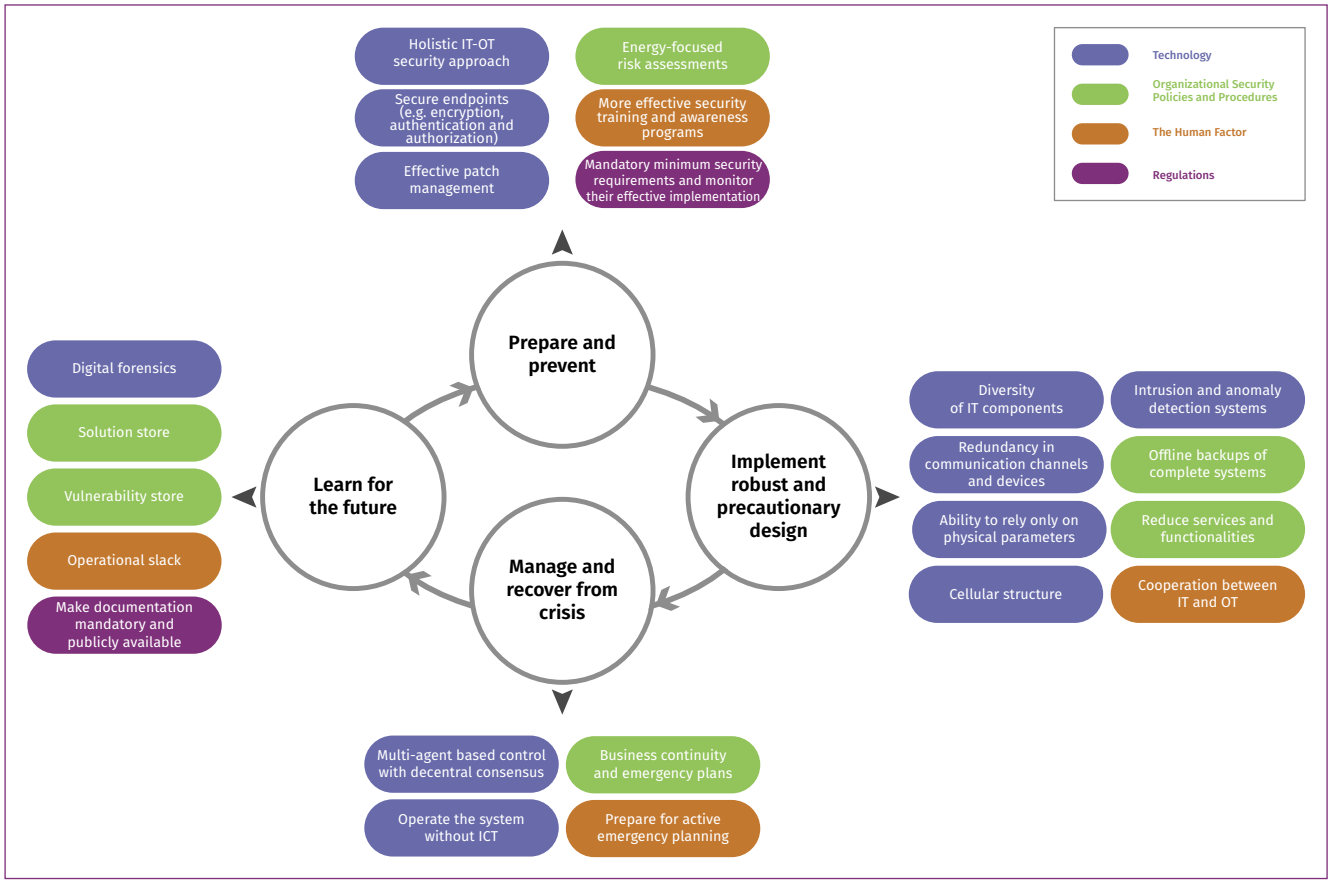

Fig. 4: Selection of resilience-enhancing measures and elements, sorted by the categories: Technology (blue), Organizational Security Policies and Procedures (green), the Human Factor (orange) and Regulations (grey), according to the Resilient Management approach phases.

Source: Authors' own compilation based on Tapia et al. (in press)

Resilience management strategy

The VA unveiled the critical vulnerable points. Security measures, if applied, have great potential to reduce some vulnerabilities. However, they focus mainly on trying to keep the malicious attackers outside of the system. Therefore, one of the biggest challenges is to find a way to broaden the horizon in handling known and unknown stressors by including recovering, adapting and learning mechanism after successful attacks, instead of only focusing on prevention and detection. This is the objective of the second part of the study. Our main concern is how to increase the resilience in CPPS. This requires the understanding that resilience is more than just eliminating identified vulnerabilities. The applied resilience management approach consists of four phases (Fig. 3).

During the **preparation and prevention** phase, weak points in the CPPS are identified and effective prevention measures must be derived. The focus here is on known stressors, thus a holistic security approach between IT-OT (IEC 2016), and energy-focused risk analysis and management strategies (Fischer et al. 2018) are needed. Experts also stressed the importance of scalable and regularly tested security measures at endpoints (e. g. encryption, authentication, authorization), intrusion detection systems, patch management, network segmentation, as well as more effective and engaging security trainings and awareness programs. Technology-wise, the implementation of additional measures for data storage and preserving of unused resources – operational slack – to better deal with surprises are helpful (Fischer and Lehnhoff 2018).

In order to enhance resilience, a **robust and precautionary system design should be implemented** from the beginning. This will empower the system to maintain its services even under stress or disturbances. The system should have a high diversity of IT components and redundancy in communication channels and devices (BNetzA 2019). Maintaining the ability to rely only on physical parameters for operation as well as hardware-based security are helpful. Furthermore, implementing a cellular structure in order to secure a minimum and stable power supply in case of a failing central ICT infrastructure appears beneficial (VDE 2015). Other suggestions supported by the experts are the implementation of real-time monitoring, intrusion and bad data detection schemes (Iturbe et al. 2016; McCarthy

et al. 2018), as well as periodic backups, and reducing services and functionalities in terms of data, ports, libraries, etc. (Fischer and Lehnhoff 2018).

A resilient power system is able to ride through failures in order to **manage and recover from crises.** While the stability and security in this phase could be enhanced by multi-agent based control with decentral consensus finding (Lehnhoff and Krause 2013), attention should also be paid to the ability to operate the system without ICT, i. e. manually, or to at least secure a *soft landing,* as experts stated. In addition, the provision of business continuity and emergency plans on a regional and local level, e. g. through *supplying islands* at least in and around public properties/buildings, and the preparation for active emergency planning and exercises based on realistic cyber-attacks have a high priority (Arghandeh et al. 2016).

Past and avoided disasters should be used in phase four **to learn for the future** in order to improve the adaptive capacity of the system. In this sense, digital forensic would allow to investigate incidents and near incidents in-depth and identify lessons. This should include the documentation of weaknesses that led to failures *(Vulnerability store)* (Gößling-Reisemann 2016). Furthermore, strengths that avoided crises in the past or enhanced recovery are equally worth identifying, as they form the basis for planning strategies and emergency scenarios *(Solution store)* (Gößling-Reisemann 2016). This documentation must be mandatory and publicly available.

Fig. 4 shows the summary of selected resilience-enhancing measures and elements for each phase of the resilience management approach. More details on the specific resilience management strategy described here can be found in Tapia et al. (in press).

Conclusions

In this study, critical properties, structures and elements contributing to the vulnerability of CPPS were identified. On one side, insecure communications or insecure end points, especially at the customer premises, resulted in a high vulnerability due to poor security features on the devices. On the other side, social engineering is a quickly growing security problem that enables threat agents to exploit one of the weaknesses present in every organization: the human factor. In spite of the existence of adaptation mechanisms that could minimize the impact, it was found that their implementation could be hindered by the lack of policy enforcement or the unreadiness of the involved actors to implement these measures. To address cybersecurity challenges, an integrated assessment considering physical, cyber and social perspectives is necessary. The aim is not only to try to keep attackers outside the system, but to design the system in a way that enables it to transform and adapt in order to cope with any kind of stressor. In other words, a resilience management strategy is needed that considers that resilience is more than just eliminating identified vulnerabilities. This article illustrated resilience enhancing measures assigned to the four phases of the resilience management cycle. One important measure is to establish an adequate cyber security regulation framework and monitor its effective implementation. Regarding the system architecture, a cellular structure and physical backup would build resilience in case of successful attacks. We conclude that introducing resilience principles/elements to the system and using a resilience management approach is a suitable way to prepare systems for the unexpected.

Acknowledgments

We acknowledge our beloved supervisor Prof. Dr. Stefan Gößling-Reisemann for his highly valuable insights and contributions during the research project Strom-Resilienz. We are very thankful to Prof. Dr. em. Arnim von Gleich for fruitful discussions and review of this manuscript, to Max Spengler for his support on the interview analysis, to Katja Hessenkämper, Katrina Stollmann and Cécile Pot d'or for proofreading.

Funding declaration

Project funded by the German Federal Ministry of Education and Research within the program Innovation and Technology Analysis, FKZ 16I1678.
http://www.stromresilienz.de

References

Acatech; Deutsche Akademie der Naturforscher Leopoldina e. V.; Akademienunion; Union der deutschen Akademien der Wissenschaften e. V. (2017): Das Energiesystem resilient gestalten. Maßnahmen für eine gesicherte Versorgung. Berlin: Acatech, Leopoldina, Akademienunion.

Arghandeh, Reza; Meier, Alexandra von; Mehrmanesh, Laura; Mili, Lamine (2016): On the definition of cyber-physical resilience in power systems. In: Renewable and Sustainable Energy Reviews 58, pp. 1060–1069.

BNetzA – Bundesnetzagentur (2019): Aktualisierung Sicherheitsanforderungen. Available online at https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/KatalogSicherheitsanforderungen/aktualisierung_sicherheitsanforderungen/aktualisierung_sicherheitsanforderungen-node.html, last accessed on 20. 12. 2019.

Bodungen, Clint; Singer, Bryan; Hilt, Stephen; Shbeeb, Aaron; Wilhoit, Kyle (2017): Hacking exposed industrial control systems. ICS and SCADA security secrets and solutions. New York: McGraw-Hill Education.

Brand, Urte et al. (2017): Resiliente Gestaltung des Energiesystems am Beispiel der Transformationsoptionen „EE-Methan-System" und „Regionale Selbstversorgung". Schlussbericht des vom BMBF geförderten Projektes RESYSTRA. Bremen: Universität Bremen. DOI: 10.2314/KXP:1667649884.

Dragos Inc. (2017): Crashoverride. Analyzing the threat to electric grid operations. Available online at https://dragos.com/blog/crashoverride/CrashOverride-01.pdf, last accessed on 21. 01. 2020.

ENISA – The European Network and Information Security Agency (2012): Smart grid security. Security related standards, guidelines and regulatory documents. Available online at https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/smart-grids/smart-grids-and-smart-metering/smart-grid-security-related-standards-guidelines-and-regulatory-documents/view, last accessed on 21. 01. 2020.

Fischer, Lars; Lehnhoff, Sebastian (2018): IT-Security for functional resilience in energy systems. In: Matthias Ruth and Stefan Goessling-Reisemann (eds.):

Handbook on resilience of socio-technical systems. Croydon: Edward Elgar Publishing Limited, pp. 316–340.

Fischer, Lars; Uslar, Mathias; Morrill, Doug; Döring, Michael; Haesen, Edwin (2018): Study on the evaluation of risks of cyber-incidents and on costs of preventing cyber-incidents in the energy sector. Final Report. Available online at https://ec.europa.eu/energy/sites/ener/files/evaluation_of_risks_of_cyber-incidents_and_on_costs_of_preventing_cyber-incidents_in_the_energy_sector.pdf, last accessed on 21. 01. 2020.

Gleich, Arnim von; Gößling-Reisemann, Stefan; Stührmann, Sönke; Woizeschke, Peer; Lutz-Kunisch, Birgitt (2010): Resilienz als Leitkonzept. Vulnerabilität als analytische Kategorie. In: Klaus Fichter, Arnim von Gleich, Reinhard Pfriem and Bernd Siebenhüner (eds.): Theoretische Grundlagen für erfolgreiche Klimaanpassungsstrategien. Delmenhorst: Projektkonsortium ‚nordwest2050', pp. 13–49.

Goessling-Reisemann, Stefan; Thier, Pablo (2019): On the difference between risk management and resilience management for critical infrastructures. In: Matthias Ruth and Stefan Goessling-Reisemann (eds.): Handbook on resilience of socio-technical systems. Croydon: Edward Elgar Publishing Limited, pp. 117–135.

Gößling-Reisemann, Stefan (2016): Resilience. Preparing energy systems for the unexpected. In: Igor Link and Valentine Florin (eds.): IRGC Resource Guide on Resilience. Lausanne: EPFL International Risk Governance Center.

Gößling-Reisemann, Stefan; Wachsmuth, Jakob; Stührmann, Sönke; Gleich, Arnim von (2013): Climate change and structural vulnerability of a metropolitan energy system. The case of Bremen-Oldenburg in Northwest Germany. In: Journal of Industrial Ecology 17 (6), pp. 846–858.

IEC – International Electrotechnical Commission (2016): Power systems management and associated information exchange. Data and communications security. Part 12: Resilience and security recommendations for power systems with distributed energy resources (DER) cyber-physical systems. 1.0. Geneva: IEC.

Iturbe, Mikel; Camacho, Jose; Garitano, Iñaki; Zurutuza, Urko; Uribeetxeberria, Roberto (2016): On the feasibility of distinguishing between process disturbances and intrusions in process control systems using multivariate statistical process control. In: Proceedings of the 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshop, pp. 155–160.

Jesse, Bernhard-Johannes; Heinrichs, Heidi; Kuckshinrichs, Wilhelm (2019): Adapting the theory of resilience to energy systems. A review and outlook. In: Energy, Sustainability and Society 9 (1), p. 27. DOI: 10.1186/s13705-019-0210-7.

Lee, Changmin; Zappaterra, Luca; Choi, Kwanghee; Choi, Hyeong-Ah (2014): Securing smart home. Technologies, security challenges, and security requirements. Proceedings of the 2014 IEEE Conference on Communications and Network Security. San Francisco: IEEE, pp. 67–72. DOI: 10.1109/CNS.2014.6997467.

Lehnhoff, Sebastian; Krause, Olav (2013): Agentenbasierte Verteilnetzautomatisierung. In: Peter Göhner (ed.): Agentensysteme in der Automatisierungstechnik. Berlin: Xpert.press Springer-Verlag, pp. 207–223.

Maynard, Peter; Mclaughlin, Kieran; Haberler, Berthold (2014): Towards understanding man-in-the-middle attacks on IEC 60870-5-104 SCADA Networks. Proceedings of the 2nd International Symposium for ICS & SCADA Cyber Security Research, pp. 30–42. Swindon, U. K.: BCS Learning & Development.

Mayring, Philipp (2014): Qualitative content analysis. Theoretical foundation, basic procedures and software solution. Available online at https://nbn-resolving.org/urn:nbn:de:0168-ssoar-395173, last accessed on 21. 01. 2020.

McCarthy, James et al. (2018): Securing manufacturing industrial control systems. Behavioral anomaly detection. NISTIR 8219. Gaithersburg: National Institute of Standards and Technology. Available online at https://www.nccoe.nist.gov/sites/default/files/library/mf-ics-nistir-8219.pdf, last accessed on 21. 01. 2020.

McLaughlin, Kieran; Friedberg, Ivo; Kang, BooJoong; Maynard, Peter; Sezer, Sakir; McWilliams, Gavin (2015): Secure communications in smart grid. Networking and protocols. In: Smart Grid Security Book 2015, pp. 113–148.

NIST – National Institute of Standards and Technology Interagency (2014): Guidelines for smart grid cybersecurity. Vol. 1: Smart Grid cybersecurity strategy, architecture, and high-level requirements. Report 7628 Rev. 1. Gaithersburg: National Institute of Standards and Technology. DOI: 10.6028/NIST.IR.7628r1.

Rossebo, Judith; Wolthuis, Reinder; Fransen, Frank; Bjorkman, Gunnar; Medeiros, Nuno (2017): An enhanced risk-assessment methodology for smart grids. In: Computer 50 (4), pp. 62–71.

Sobczak, Blake (2019): Experts assess damage after first cyberattack on U. S. grid. Security. In: E & E News. Available online at https://www.eenews.net/stories/1060281821, last accessed on 21. 01. 2020.

Styzcynski, Jake; Beach-Westmoreland, Nate (2019): When the lights went out. A comprehensive review of the 2015 attacks on Ukrainian critical infrastructure. n. p.: Booze Allen Hamilton Inc. Available online at https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf, last accessed on 21. 01. 2020.

Tapia, Mariela; Thier, Pablo; Gößling-Reisemann, Stefan (in press): artec Paper No. 222: Vulnerability and resilience of cyber-physical power system. Results from an empirical-based study.

VDE – Verband der Elektrotechnik Elektronik und Informationstechnik (2015): Der Zellulare Ansatz. Grundlage einer erfolgreichen, regionenübergreifenden Energiewende. Frankfurt a. M.: VDE ETG.

MARIELA TAPIA

holds a M. Sc. in Renewable Energy. Since 2016, she is working as research associate in the research group *Resilient Energy Systems* at the University of Bremen. Her research focus is resilient transformation of power supply in developing countries.

PABLO THIER

has a background in experimental physics. Since 2015, he has been working in different projects at the University of Bremen in the research group *Resilient Energy Systems,* where he is developing a framework for making resilient decisions for energy systems.

PROF. DR. RER. NAT. STEFAN GÖßLING-REISEMANN (1968–2018)

was a theoretical physicist. He was the chair of the research group *Resilience Energy System* and the speaker of the *Advanced Energy Systems Institute* at the University of Bremen. His research aimed at solving the substantial problems of this planet. His last projects aimed at designing resilient and sustainable energy systems.